UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Seizure of Eighteen (18) ".Com" Domain Names, further described in Attachment A	)))))	Case No. 4:22MJ6246 PLC

APPLICATION AND AFFIDAVIT FOR SEIZURE WARRANT

I, Peter Dyer, being duly sworn depose and say:

I am a Postal Inspector with the United States Postal Inspection Service, and have reason to believe that there is now certain property namely

Eighteen (18) ".Com" Domain Names, further described in Attachment A

which is

subject to forfeiture under Title 18, United States Code, Sections 981(a) & 982(a) & 1028(b) & 1029(c) and Title 28, United States Code, Section 2461, and therefore, is subject to seizure under Title 18, United States Code, Sections 981(b) & 982(b) and Title 21, United States Code, Sections 853(e)&(f) concerning a violation of Title 18, United States Code, Sections 1028, 1029, 1341, 1343, and 1349.

The facts to support a finding of Probable Cause for issuance of a Seizure Warrant are as follows:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

Continued on the attached sheet and made a part hereof. X **Yes** ____ **No**

Signature of Affiant, Postal Inspector Peter Dyer

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41

October 21, 2022
Date and Time Issued

at St. Louis, Missouri
City and State

Honorable Patricia L. Cohen, U.S. Magistrate Judge
Name and Title of Judicial Officer

Patricia L. Cohen
Signature of Judicial Officer

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	Case No.: 4:22MJ6246 PLC
EIGHTEEN (18) ".COM"	)	**Filed Under Seal**
DOMAIN NAMES	)	

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Peter Dyer, being duly sworn, hereby declare as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Postal Inspector with the United States Postal Inspection Service (hereinafter "USPIS") and I have ten (10) years of federal law enforcement experience. I am currently assigned to work financial fraud schemes. I am also assigned to the FBI's Cyber Task Force where I investigate offenses relating to the use of computers, networks, and technology in the commission of crimes. I am authorized by law or by a government agency to engage in or supervise the prevention, detention, investigation, or prosecution of a violation of Federal criminal laws.

2. I have learned how to conduct such investigations through previous investigations, formal training, and in consultation with law enforcement partners in local, state, and federal law enforcement agencies. I have been trained to investigate federal crimes and have investigated an array of complex federal crimes.

3. In these investigations, I have been involved in the application for and execution of numerous arrest and search warrants related to the aforementioned criminal offenses. Through my training and experience, I am familiar with the actions, habits, traits, methods, and terminology utilized by criminal offenders.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PURPOSE OF APPLICATION

5. I submit this application in support of seizure warrants for eighteen (18) domain names, as detailed in Attachment A, hereafter referred to as SUBJECT DOMAIN NAMES, as property used or intended to be used to commit or to facilitate the commission of violations of 18 U.S.C. §§ 1028 (identity theft), 1028A (aggravated identity theft), 1029 (access device fraud), 1349 (conspiracy to commit mail and wire fraud), 1341 (mail fraud) and 1343 (wire fraud) (SUBJECT OFFENSES), and are therefore subject to seizure pursuant to 21 U.S.C. § 853(f) and 18 U.S.C. §§ 1028(g) and 1029(c)(2). The procedure by which the government will seize the SUBJECT DOMAIN NAMES are described in Attachment B hereto and below.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

6. Pursuant to Title 18, United States Code, Section 1028(b)(5), any personal property used or intended to be used to commit the offense of Identity Theft is subject to criminal forfeiture.

7. In addition, pursuant to Title 18, United States Code, Section 1029(c)(1)(C), any personal property used or intended to be used to commit the offense of Access Device Fraud is subject to criminal forfeiture.

8. This application seeks a seizure warrant under criminal authority because the property to be seized could be placed beyond process if not seized by warrant.

9. Pursuant to both 18 U.S.C. §§ 1028(g) and 1029(c)(2), the procedures in 21

U.S.C. § 853 (other than subsection (d)) govern this criminal forfeiture action. 21 U.S.C. § 853(f) provides authority for the issuance of a seizure warrant for property subject to criminal forfeiture in the same manner as provided for a search warrant. Additionally, 21 U.S.C. § 853(1) grants jurisdiction to this Court without regard to the location of any property which may be subject to forfeiture.

10. Based on the foregoing, the issuance of this seizure warrant is authorized under 21 U.S.C. § 853(f) and 18 U.S.C. §§ 1028(g) and 1029(c)(2) for criminal forfeiture.

11. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the SUBJECT DOMAIN NAMES for forfeiture. By seizing the SUBJECT DOMAIN NAMES and redirecting them to another website, the Government will prevent third parties from acquiring the name and using it to commit additional crimes. Furthermore, seizure of the SUBJECT DOMAIN NAMES will prevent third parties from continuing to access the SUBJECT DOMAIN NAMES and their corresponding websites in their present form.

12. As set forth above, there is probable cause to believe that the SUBJECT DOMAIN NAMES are subject to criminal forfeiture because they were used in the commission of violations of the SUBJECT OFFENSES. Specifically, the SUBJECT DOMAIN NAMES were used or intended to be used to commit identity theft and access device fraud.

BACKGROUND ON DOMAIN NAMES

13. Based on my training and experience and information learned from others, I am aware of the following:

a. Internet Protocol Address: An Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to

the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address -- it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs.

b. Domain Name: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

c. Domain Name System: The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain. For example, the domain name "www.example.com" means that the computer assigned that name is in the ".com" top-level domain, the "example" second-level domain, and is the web server.

d. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into Internet Protocol ("IP") addresses.

e. Registry: For each top-level domain (such as ".com"), there is a single company, called a "registry," that determines which second-level domain resolves to which IP address. For example, the registry for the ".com" and ".net" top-level domains are VeriSign, Inc., which has its headquarters at 12061 Bluemont Way, Reston, Virginia.

f. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The individual or business that purchases, or registers, a domain name is called a "registrant." Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Typically, a registrar will provide a registrant with the ability to change the IP address a particular IP address resolves through an online interface. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

g. WHOIS: A "WHOIS" search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A WHOIS record for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range and domain name. For example, a WHOIS record for the domain name XYZ.COM might list an IP address range of 12.345.67.0-12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0-12.345.67.99.

TRAINING AND EXPERIENCE OF THE INVESTIGATIVE TEAM

14. Based on my knowledge, training, and experience, and information I learned from others, I know that:

a. Fraud schemes that utilize false job postings advertising "work-at-home" employment and manipulate job seekers into unknowingly participating in criminal conduct or transactions, are known as Work-at-home Scams.

b. Work-at-home scams that manipulate job seekers into receiving stolen goods, merchandise, or money and reshipping it to another address controlled by the scammers, are known as Reshipping Scams. The goods and merchandise reshipped in these scams are often the result of identity theft and credit card fraud.

c. Reshipping scams lure job seekers by utilizing a false narrative that creates rapport and deceives victims into believing they are accepting a job with a legitimate company and performing a legitimate job function. Many times, scammers require the job seeker to fill out forms customarily used during a legitimate hiring process, such as IRS Form W-4 and direct deposit information.

d. Reshipping scammers utilize false personas to portray additional roles at the fictional company to further their deception. This may include emails to the victim from purported employees of the fictional company's Human Resources or Shipping departments.

e. After developing rapport, scammers direct the job-seeker, now unwitting participant and witness, to create and utilize online credentials to access the fictional company's domain. This domain is commonly referred to by the scammers as a "dashboard." The dashboard enables the witness to communicate with the scammers electronically, thereby eliminating the need for face-to-face or verbal communication.

f. The dashboard serves as the sole means for the witness to view incoming shipments, acknowledge receipt of the shipment, upload a photograph of the received shipment, request a new label, acknowledge reshipment of the item(s), and provide the scammers with the new tracking number.

g. Reshipping scammers often use vulnerable witnesses to unwittingly conduct these transactions in order to avoid law enforcement detection and put layers between themselves and

the stolen merchandise or other fraud proceeds.

h. Reshipping scammers often impose a sense of urgency and require the witness to complete these steps within a short time period, often twenty-four hours or less, in order to evade detection or interception by law enforcement.

i. Reshipping scammers often use numerous fictional company names, addresses, and domains in order to avoid detection by law enforcement and thwart negative news posted online by previous witnesses and victims.

j. Once a fictional company name is exposed for being involved in a scam, reshipping scammers often utilize variations of their fictious company names in order to avoid detection by law enforcement and thwart negative news posted online by witnesses and victims.

k. Reshipping scammers often use multiple aliases, email addresses, usernames, log-in credentials, IP addresses, and other unique identifiers in order to communicate with scheme participants, conceal their true identity, and avoid detection by law enforcement.

l. Reshipping scams utilize a means of identification, to include but not limited to; victim's names and credit card information, reshipper's names and address, and employee's names, without lawful authority to facilitate the receipt and reshipment of stolen goods.

CASE BACKGROUND

15. In February 2021, Victim "D.S." identified a fraudulent charge to his American Express account which resulted in the merchandise being shipped to an address in St. Louis County, Missouri, with which he was unfamiliar. "D.S." reported this information to the United States Postal Service Office of Inspector General, who conducted a preliminary investigation and then forwarded the information to the U.S. Postal Inspection Service.

16. In March 2021, I interviewed "D.S.", a resident of St. Louis County, Missouri, and learned the following:

a. "D.S." received an email regarding an unauthorized purchase from Dell.com for $769.26 from his American Express credit card,

b. "D.S." was in physical possession of his American Express card and did not make or authorize this purchase,

c. "D.S." informed American Express and Dell that he did not make the purchase,

d. "D.S." learned the merchandise was shipped to an address in St. Louis County, Missouri with which he was unfamiliar (hereinafter referred to as "Hazelwood Address"), and

e. "D.S." learned the order was associated with a phone number with which he was not familiar.

17. I reviewed Dell records associated with the aforementioned unauthorized purchase which showed an unknown person ordered a virtual-reality headset and requested that it be shipped via commercial carrier expedited service to the Hazelwood Address.

18. I researched the Hazelwood Address and identified it was a single-family residential home in St. Louis County, Missouri, located within the Eastern District of Missouri.

19. Based on this information, I determined "D.S." was a victim of identity theft and credit card fraud based on the use of his means of identification without lawful authority.

20. I identified the Hazelwood Address was occupied by "D.L." In March 2021, I interviewed "D.L." and learned the following:

a. Because of the COVID-19 pandemic, "D.L." sought and obtained work-from-home employment as a Quality Control Inspector with Local Post for International Customers, LLC or "LocalPost",

b. "D.L." was instructed by LocalPost to receive packages at her Hazelwood Address, photograph the package and its contents, and then reship the items to another address using a shipping label provided by LocalPost,

c. "D.L." communicated with LocalPost using email and through the messaging system on the company's dashboard domain LOCALPOST-US.COM,

d. "D.L." never spoke to anyone at LocalPost in-person, over the phone, or via live video chat,

e. "D.L." was instructed to visit the domain LOCALPOST-US.COM daily and log-in with her username and password,

f. "D.L." requested tasks, or jobs, using LOCALPOST-US.COM,

g. Within a day or two of requesting a task, "D.L." received a package at her residence. The packages were shipped via United States Postal Service (hereinafter "USPS") and commercial carriers.

h. "D.L." was instructed to photograph the package and shipping label and upload the photograph to LOCALPOST-US.COM,

i. In some instances, "D.L." was instructed to open the package, photograph the contents of the package, and then repackage the contents in another box,

j. "D.L." would download a new shipping label from LOCALPOST-US.COM,

k. "D.L." would apply the new label,

l. "D.L." was instructed to ship the package via USPS or commercial carrier to the new address.

m. "D.L." was then instructed to photograph a copy of the shipment receipt and upload it to LOCALPOST-US.COM,

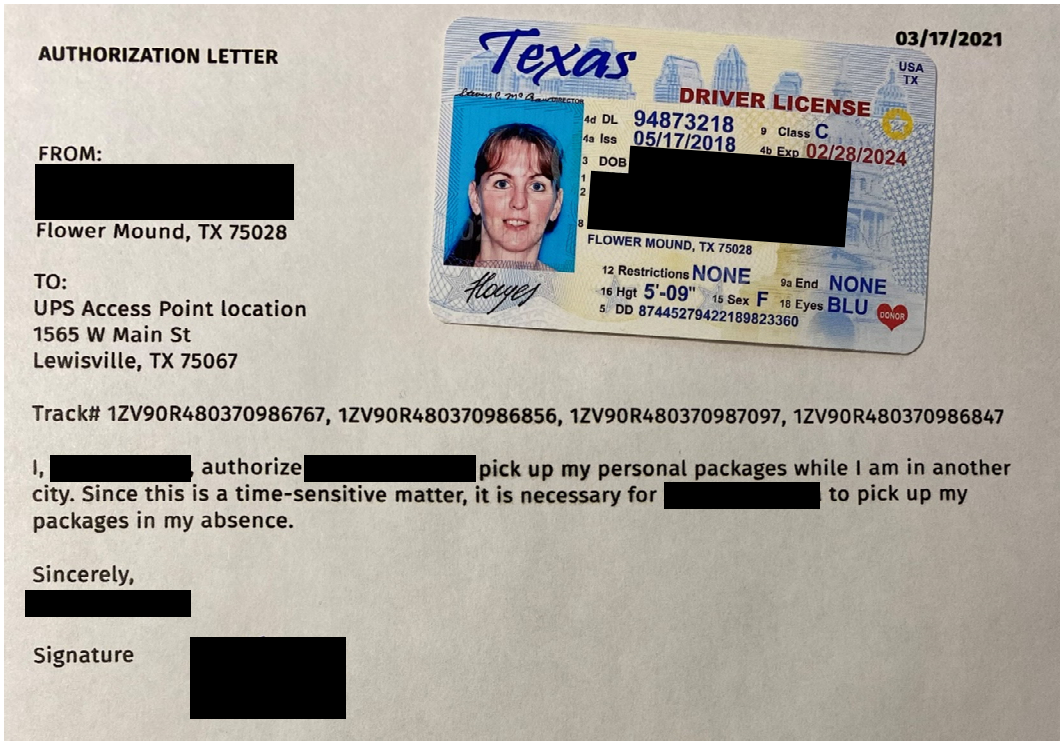
n. Upon completion of all of these steps, "D.L." would earn $20.00 per package,

o. "D.L." received her earnings through a deposit into her PayPal account, and

p. "D.L." completed 9 tasks and was paid a total of $180.00 by LOCALPOST.

21. On or about March 18, 2021, I observed "D.L." log-in to LOCALPOST-US.COM and scroll through the domain's options. I also observed a historical list of packages "D.L." received and reshipped, to include but not limited to the package which contained items purchased using the credit card of Victim "D.S."

22. On or about March 18, "D.L." forwarded an email message she received from LocalPost instructing her to pick up a package. This email contained a photograph attachment. This photograph appeared to be sent to "D.L." in error because it contained a written statement referencing individuals, addresses, and packages with which she was unfamiliar, as shown in the photograph below:



23. Using the Texas Driver's License information from above, I queried law enforcement databases and learned the identification number is not on file and the photograph and date of birth are not correct for the individual named at that address.

24. Based on my knowledge, training, and experience, I believe this photograph attachment was sent to "D.L." in error and was meant to be sent to another "Quality Control Inspector" in Texas who was being instructed by LocalPost to pick up packages addressed to the name portrayed on the invalid Texas Driver's License.

25. Based on this information, I determined R.H. was a victim of identity theft based on the use of her means of identification without lawful authority.

26. During this same timeframe, "D.L." stated she was contacted by Hazelwood Police Department regarding a package containing stolen merchandise shipped to her residence. When Hazelwood Police learned the matter was being investigated by the U.S. Postal Inspection Service, they stopped any further law enforcement action.

27. On April 15, 2021, I received and reviewed Hazelwood Police records which showed they received a phone call from "J.F." who reported his credit card was used without his permission to purchase a $1,500 laptop which was shipped to the Hazelwood Address.

28. In April 2021, I contacted "J.F.", a resident of St. Louis County, Missouri, and learned the following:

a. "J.F." received an email regarding an unauthorized purchase of approximately $1,500 from his eBay account, which was linked to his Chase credit card,

b. "J.F." did not make or authorize this purchase,

c. "J.F." informed eBay and Chase that he did not make the purchase,

d. "J.F." learned the laptop was shipped to the Hazelwood Address, and

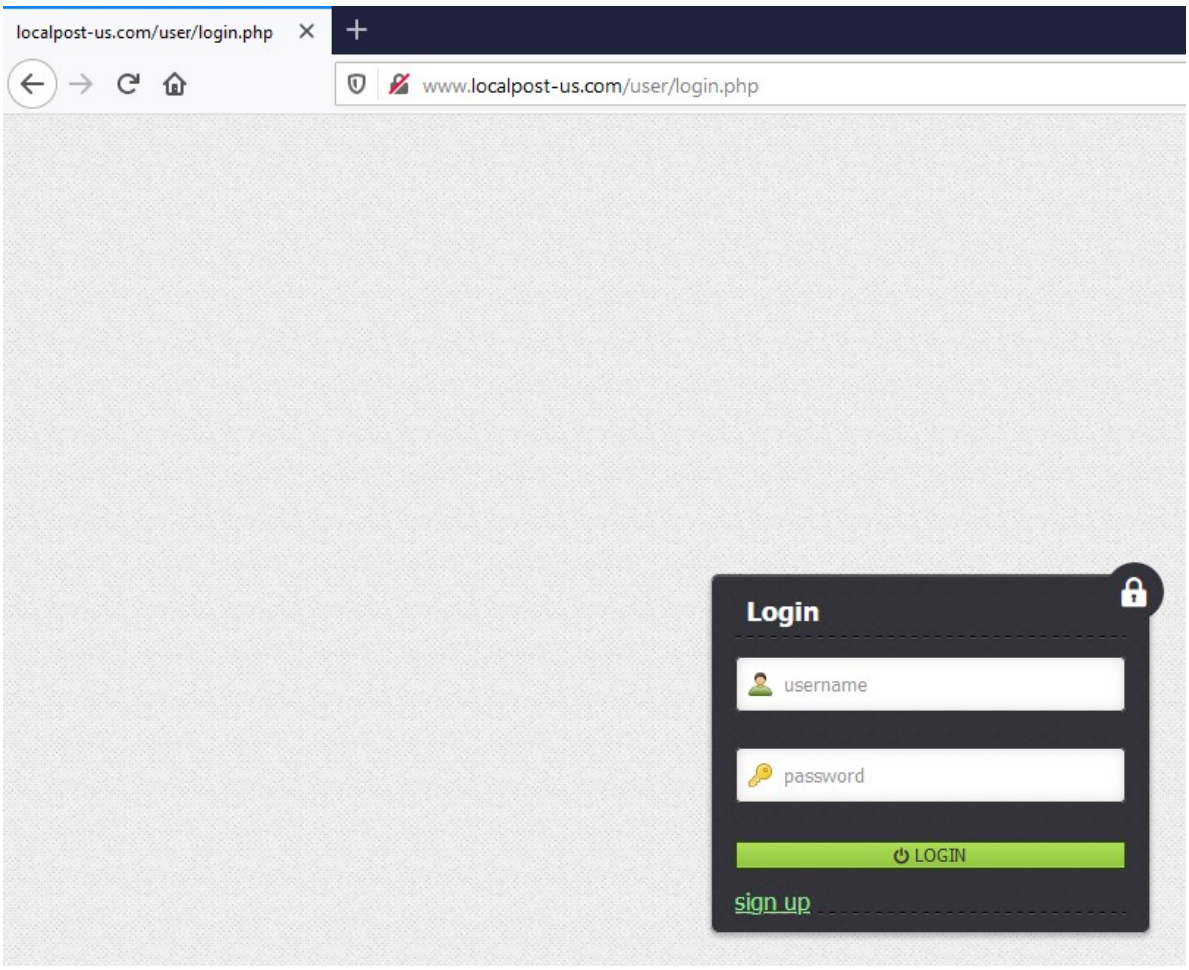
e. "J.F." is not familiar with the Hazelwood Address.

29. Based on this information, I determined "J.F." was a victim of identity theft and credit card fraud based on the use of his means of identification without lawful authority.

Consent to Assume Online Identity

30. On or about March 19, 2021, "D.L." provided written consent for law enforcement to assume her online identity associated with LOCALPOST-US.COM and provided her username and password.

31. On or about March 19, 2021, based on the written consent of "D.L.", I went to the domain LOCALPOST-US.COM and observed the following dashboard control panel screen, as shown in the figure below:

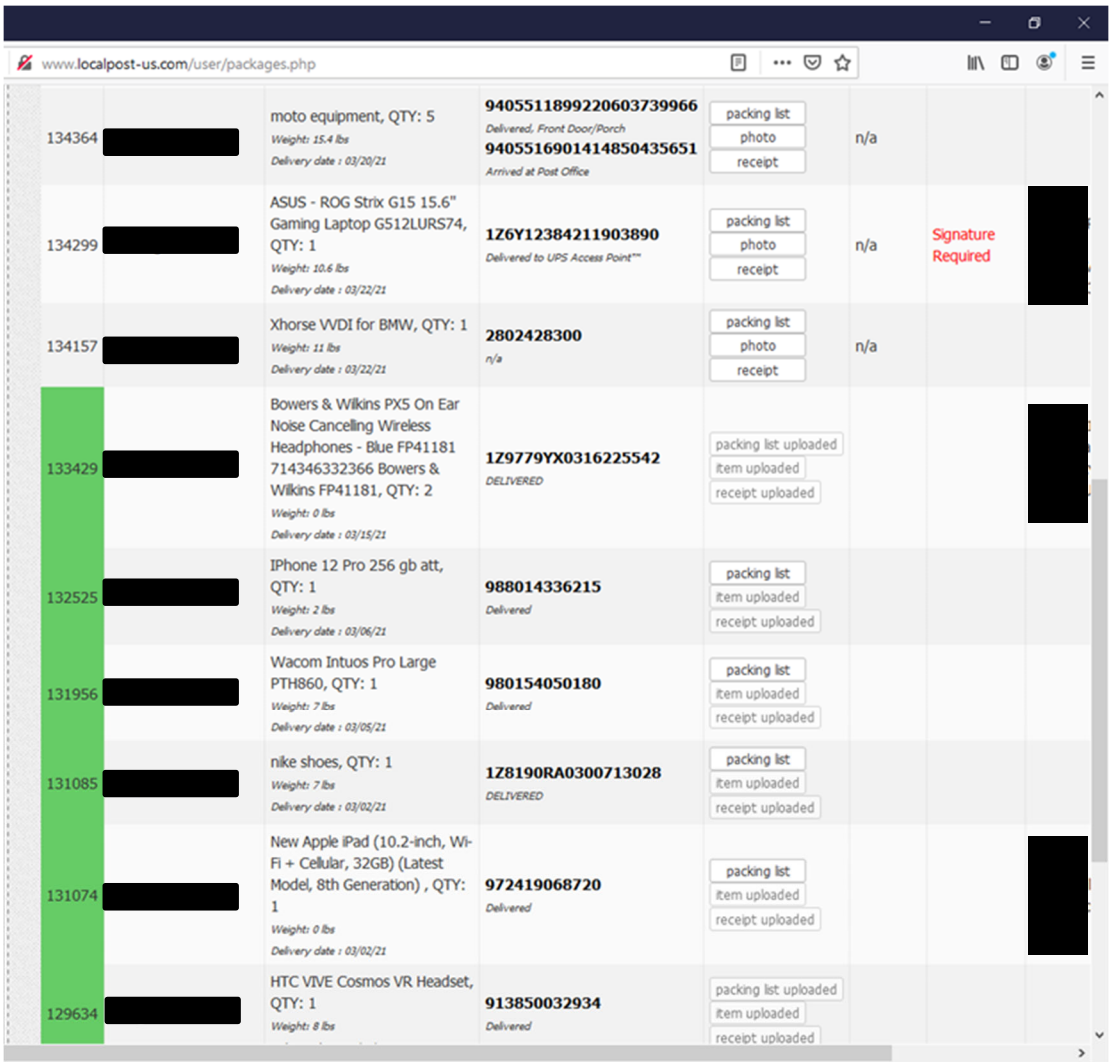


1 *Local Post Dashboard; March 19, 2021*

32. I entered the username and password of "D.L." I observed the domain LOCALPOST-US.COM had navigation links labeled: Home, News, Scanned Documents, Packages, Help, Mail, Settings, My Profile, Stats, and Request money.

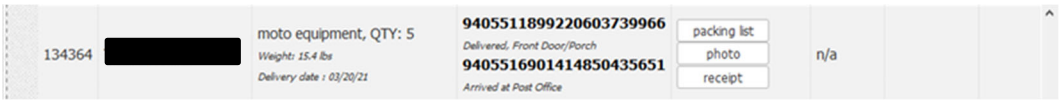
33. I selected the Packages link, was taken to the url WWW.LOCALPOST-US.COM/USER/PACKAGES.PHP, and observed the following, to include but not limited to:

a. At least twenty-five (25) package tracking numbers from USPS and commercial carriers arranged in columns listing the addressee's name, package contents, tracking numbers, upload links, status, and other information, as shown in the redacted photograph below:



2 *WWW.LOCALPOST-US.COM/USER/PACKAGES.PHP*

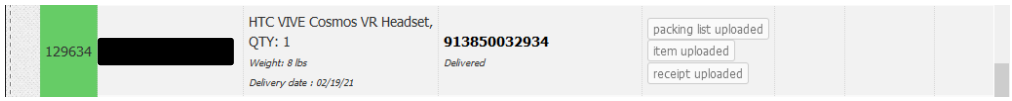
b. A USPS package with label 9405511899220603739966, the name "T.B.", description "moto equipment QTY: 5", and notes "Delivered, Front Door/Porch", as shown in the redacted photograph below, and the same as the package I received from "D.L." on or about March 19, 2021:



3 WWW.LOCALPOST-US.COM/USER/PACKAGES.PHP

c. A USPS package with label 9405516901414850435651, the name "T.B.", description "moto equipment QTY: 5", and notes "Arrived at Post Office", as shown in the photograph above,

d. A commercial carrier package with label 913850032934, the same name of "D.S.", the victim described in paragraphs 8 and 9 above, description "HTC VIVE Cosmos VR Headset, QTY:1", and notes "Delivered", as shown in the redacted photograph below:



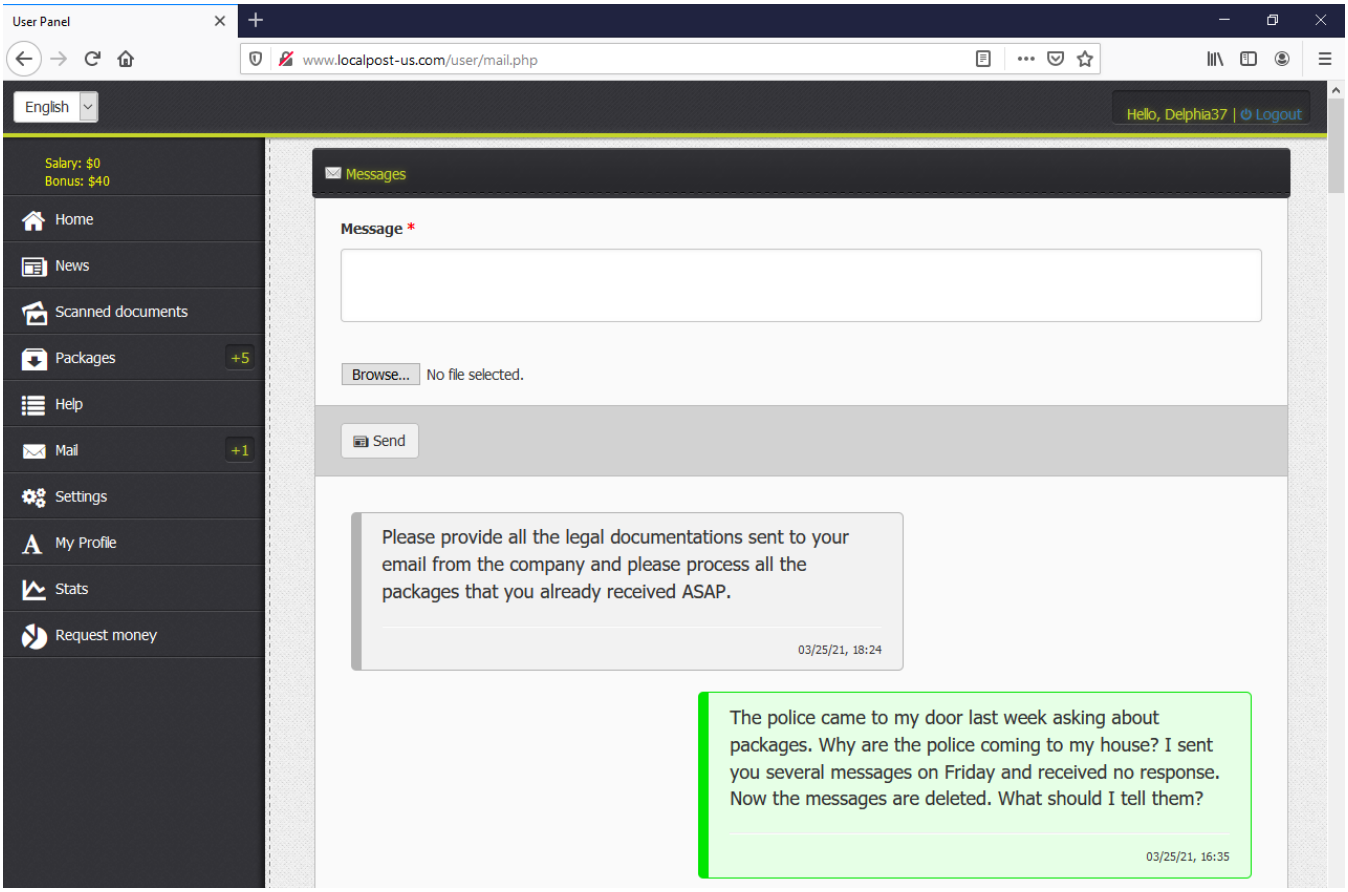
4 WWW.LOCALPOST-US.COM/USER/PACKAGES.PHP

e. A commercial carrier package with label 1Z6Y12384211903890, the same name of "J.F.", the victim described in paragraphs 18 and 19 above, description "ASUS…", and notes "Delivered to UPS Access Point", as shown in the redacted photograph below:

5 WWW.LOCALPOST-US.COM/USER/PACKAGES.PHP

34. I selected the Mail link, was taken to the url WWW.LOCALPOST-US.COM/USER/MAIL.PHP, and observed messages between "D.L." and unknown persons coordinating the shipment of packages, uploading of photographs, and sharing of labels.

35. Between March 19, 2021 and March 25, 2021 I logged onto LOCALPOST-US.COM using the username and password of "D.L." and attempted to communicate via text message with the unknown persons operating the dashboard with negative results. On March 25, 2021 at 1:24pm CST, I communicated via text with an unknown person operating the dashboard. My communication is highlighted in green and the unknown person's response is highlighted in grey, as shown in the photograph below:



6 WWW.LOCALPOST-US.COM/USER/MAIL.PHP

36. On March 26, 2021, I was contacted by "D.L." who stated she received an email from someone purporting to be L.N., LocalPost Manager Shipping Department, who was threatening legal action if "D.L." did not reship packages as she was instructed to do so.

37. Postal records show an unknown individual tracked USPS package 9405511899220603739966 from IP addresses that originated from Russia on at least fourteen occasions.

38. Postal records show an unknown individual tracked USPS package 9405516901414850435651 from IP addresses that originated from Russia on at least thirty-two occasions.

39. Grand Jury subpoena records and returns from PayPal regarding the account of "D.L." show two deposits that correspond to statements made by "D.L." that she received compensation from LOCALPOST through deposits into her PayPal account. These PayPal records showed:

a. The first payment to "D.L." occurred on March 1, 2021, and was sent from a PayPal account with a user name of "Y[redacted] K[redacted]" and the email address K[redacted].Y[redacted]@GMAIL.COM.

b. The second payment to "D.L." occurred on March 6, 2021, and was sent from a PayPal account with the user name of "A[redacted] A[redacted]", the email address G[redacted]@YANDEX.RU, and a shipping address in Russia.

40. Based on my knowledge, training, and experience I believe these PayPal accounts which made payments to "D.L." are associated with unknown subjects who originated from or are utilizing account and addresses associated with or located in Russia.

41. Grand Jury subpoena records and returns from Google associated with K[redacted].Y[redacted]@GMAIL.COM showed the following:

a. The account was created on April 22, 2014, using IP address 87.244.157.244, and

b. The recovery email address for this account is K[redacted]-Y[redacted]@MAIL.RU.

42. I conducted open-source research of IP address 87.244.157.244 and learned it is managed by Satellite Ltd., an internet service provider based in Ukraine.

43. I conducted open-source research of Mail.RU and learned it is an email service provider based in Russia.

44. I conducted open-source research of LOCALPOST-US.COM and learned the domain was associated with the following registrant contact information: S[redacted] L[redacted], [redacted], Matteson, IL 60443, ([redacted]) [redacted], and S[redacted]@MAIL.COM.

45. Grand Jury subpoena records and returns from 1&1 Media showed S[redacted]@MAIL.COM was associated with the alternate email address Y[redacted]@EMAIL.COM and the IP address 208.103.76.239 on April 9, 2020.

46. I conducted open-source research of IP address 208.103.76.239 and identified it was associated with the internet service provider Atlantic Broadband.

47. Grand Jury subpoena records and returns from Atlantic Broadband showed IP address 208.103.76.239 on April 9, 2020, was associated with a gas station in Waterford, Connecticut.

48. I conducted open-source research of LOCALPOST-US.COM and learned the domain was associated with computer servers at Cloudflare.

Cloudflare Records

49. Grand Jury subpoena records and returns from Cloudflare revealed the domain LOCALPOST-US.COM was associated with an unknown user with the email address W[redacted]@MAIL.RU and the IP address 185.248.101.120.

50. Cloudflare records also revealed the unknown user with the email address W[redacted]@MAIL.RU utilized Cloudflare to reroute internet traffic from the thirty-six (36) domains that end with ".com, as shown in the chart below:

account-cargill.com	dash-orient.com	sa-dash.com
account-navois.com	dash-satori.com	sa-dashboard.com
amari-dash.com	dash-spt.com	satori-dash.com
cargill-account.com	egreen-dash.com	scorpio-control.com
century-dash.com	e-warehouses.com	sg-dashboard.com
control-scorpio.com	fastpsonia-dash.com	sgl-dash.com
costa-account.com	lagoon-dash.com	sp-dashboard.com
dash-amari.com	localpost-us.com	spt-dash.com
dashboard-zim.com	main-dashboard.com	syntax-dash.com
dash-cp.com	main-sgl.com	zim-dash.com
dash-egreen.com	navois-account.com	
dash-fastpsonia.com	orient-dash.com	
dash-lagoon.com	patrol-dash.com	

51. This includes the eighteen SUBECT DOMAIN NAMES and eighteen other domains with the same content, word sequence, and functionality. These additional eighteen domains that are not included as SUBJECT DOMAIN NAMES have been suspended or are no longer active.

52. The SUBJECT DOMAIN NAMES are identified below, and included in Attachment A:

account-navois.com	dash-egreen.com	navois-account.com
amari-dash.com	dash-orient.com	orient-dash.com
control-scorpio.com	dash-satori.com	satori-dash.com
costa-account.com	dash-spt.com	scorpio-control.com
dash-amari.com	egreen-dash.com	spt-dash.com
dashboard-zim.com	main-sgl.com	zim-dash.com

53. Cloudflare records also showed that as of March 2, 2022, the SUBJECT DOMAIN NAMES controlled by user W[redacted]@MAIL.RU were still active.

54. The creation dates for the SUBJECT DOMAIN NAMES range from February 17, 2021, when LOCALPOST-US.COM and five other domains were created, to January 26, 2022, when two domains were created.

55. The SUBJECT DOMAIN NAMES controlled by user W[redacted]@MAIL.RU were directing internet traffic to IP addresses in Russia, Latvia, Poland, and Cyprus.

Open-Source Research

56. On April 14, 2022, I conducted research using a publicly available internet browser and a cellular internet connection. No special law enforcement tools or techniques were used. I entered each of the thirty-six domain names into the internet browser and observed that they directed me to a patterned address of https:/DOMAIN NAME/user/login.php, as shown in the chart below:

Ref	*DOMAIN NAME*	*Result of research*
1	account-cargill.com	https://account-cargill.com/user/login.php
2	account-navois.com	https://account-navois.com/user/login.php
3	amari-dash.com	https://amari-dash.com/user/login.php
4	cargill-account.com	https://cargill-account.com/user/login.php
5	century-dash.com	https://century-dash.com/user/login.php
6	control-scorpio.com	https://control-scorpio.com/user/login.php
7	costa-account.com	https://costa-account.com/user/login.php
8	dash-amari.com	https://dash-amari.com/user/login.php
9	dashboard-zim.com	https://dashboard-zim.com/user/login.php
10	dash-cp.com	https://dash-cp.com/user/login.php
11	dash-egreen.com	https://dash-egreen.com/user/login.php
12	dash-fastpsonia.com	https://dash-fastpsonia.com/user/login.php
13	dash-lagoon.com	https://dash-lagoon.com/user/login.php
14	dash-orient.com	https://dash-orient.com/user/login.php
15	dash-satori.com	https://dash-satori.com/user/login.php
16	dash-spt.com	https://dash-spt.com/user/login.php

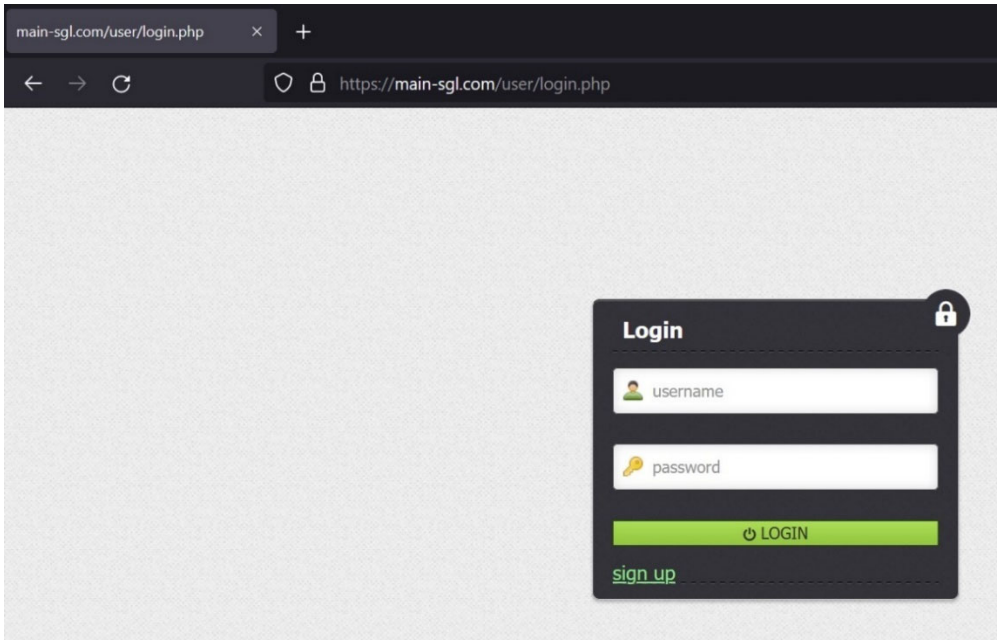
17	egreen-dash.com	https://egreen-dash.com/user/login.php
18	e-warehouses.com	https://e-warehouses.com/user/login.php
19	fastpsonia-dash.com	https://fastpsonia-dash.com/user/login.php
20	lagoon-dash.com	https://lagoon-dash.com/user/login.php
21	localpost-us.com	-
22	main-dashboard.com	-
23	main-sgl.com	https://main-sgl.com/user/login.php
24	navois-account.com	https://navois-account.com/user/login.php
25	orient-dash.com	https://orient-dash.com/user/login.php
26	patrol-dash.com	https://patrol-dash.com/user/login.php
27	sa-dash.com	https://sa-dash.com/user/login.php
28	sa-dashboard.com	https://sa-dashboard.com/user/login.php
29	satori-dash.com	https://satori-dash.com/user/login.php
30	scorpio-control.com	https://scorpio-control.com/user/login.php
31	sg-dashboard.com	https://sg-dashboard.com/user/login.php
32	sgl-dash.com	https://sgl-dash.com/user/login.php
33	sp-dashboard.com	-
34	spt-dash.com	https://spt-dash.com/user/login.php
35	syntax-dash.com	https://syntax-dash.com/user/login.php
36	zim-dash.com	https://zim-dash.com/user/login.php

57. On July 29, 2022, I again conducted research using a publicly available internet browser and a cellular internet connection. No special law enforcement tools or techniques were used. I entered each of the SUBJECT DOMAIN NAMES into the internet browser and observed that the SUBJECT DOMAIN NAMES directed me to a patterned address of https:/SUBJECT DOMAIN NAMES/user/login.php, as shown in the chart below:

Ref	***SUBJECT DOMAIN NAME***	***Result of research***
1	account-navois.com	https://account-navois.com/user/login.php
2	amari-dash.com	https://amari-dash.com/user/login.php
3	control-scorpio.com	https://control-scorpio.com/user/login.php
4	costa-account.com	https://costa-account.com/user/login.php
5	dash-amari.com	https://dash-amari.com/user/login.php
6	dashboard-zim.com	https://dashboard-zim.com/user/login.php
7	dash-egreen.com	https://dash-egreen.com/user/login.php
8	dash-orient.com	https://dash-orient.com/user/login.php
9	dash-satori.com	https://dash-satori.com/user/login.php
10	dash-spt.com	https://dash-spt.com/user/login.php
11	egreen-dash.com	https://egreen-dash.com/user/login.php

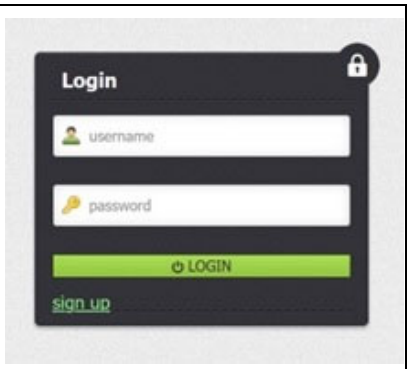
12	main-sgl.com	https://main-sgl.com/user/login.php
13	navois-account.com	https://navois-account.com/user/login.php
14	orient-dash.com	https://orient-dash.com/user/login.php
15	satori-dash.com	https://satori-dash.com/user/login.php
16	scorpio-control.com	https://scorpio-control.com/user/login.php
17	spt-dash.com	https://spt-dash.com/user/login.php
18	zim-dash.com	https://zim-dash.com/user/login.php

58. The SUBJECT DOMAIN NAMES also displayed the exact same log-in screen, or dashboard control panel, as shown in the figure below obtained from the domain main-sgl.com, one of the SUBJECT DOMAIN NAMES:



7 Dashboard of a subject domain name: main-sgl.com/user/login.php

59. These April 14, 2022, and July 29, 2022 observations show the same dashboard control panel that I observed when I visited the domain LOCALPOST-US.COM on March 21, 2021, as shown in the photographs below:

		
March 19, 2021 Screenshot from LOCALPOST-US.COM	April 14, 2022 Screenshot from MAIN-SGL.COM	July 29, 2022 Screenshot From ACCOUNT-NAVOIS.COM

8 Comparison of Subject Domain Name Dashboards

60. Based on these findings I believe that the SUBJECT DOMAIN NAMES, all with nearly identical content and sequences of words, are being used by unknown subjects to facilitate the SUBJECT OFFENSES. I further believe the eighteen domain names that are not currently active were previously used to facilitate the SUBJECT OFFENSES and are readily able to be deployed to continue to facilitate the SUBJECT OFFENSES in the immediate future.

FBI Complaints

61. The Federal Bureau of Investigation takes reports from the public concerning suspected internet-facilitated criminal activity. These reports are stored in the Internet Crime Complaint Center, or "IC3", a secure online database available only to law enforcement. IC3 records showed sixty-four (64) complaints referenced the thirty-six domain names identified in the Cloudflare records.

62. Members of the investigative team and I reviewed numerous IC3 complaints that referenced the domain names identified in the Cloudflare records, to include but not limited to, account-cargill.com and cargill-account.com. Both SUBJECT DOMAIN NAMES were reported associated with a work-at-home scam. Victim "D.M.", a resident of Washington, reported the following:

a. On or about February 2022, D.M. was offered a remote job by the company Cargill Post. The company provided D.M. a domain to access the employee online dashboard, account-cargill.com, one of the domain names identified in the Cloudflare records,

b. D.M. was hired to receive packages and resend them out on the same day using an outgoing shipping label provided by the company (i.e., the victim was hired as a "reshipper").

c. D.M. provided the subject company with PII, such as name, address, and social security number,

d. D.M. was contacted from multiple email addresses that followed the naming convention "firstname(dot)lastname(at)companynameemail.com." For example, E[redacted] G[redacted] emailed D.M. from email address E[redacted](at)cargillemail.com., and

e. Before the first pay period, D.M.'s dashboard account was locked or disconnected.

63. Victim "D.J.", a resident of New Jersey, reported the following to IC3:

a. On or about January 7, 2022, D.J. was offered a remote job by the company Scorpio Group LLC. The company provided D.J. a domain to access the employee online dashboard, scorpio-control.com,

b. D.J. was hired to receive packages, then send them out on the same day using an outgoing shipping label provided by the company (i.e., the victim was hired as a "reshipper").

D.J. was told the position salary was $1600 monthly with an added $50 bonus per package delivered successfully for an average income of $3800 per month.,

c. D.J. was contacted from multiple email addresses that followed the convention firstname(dot)lastname(at)companynameemail.com. For example, D[redacted] K[redacted] emailed D.J. from email address d[redacted]@scorpiogemail.com,

d. On or about February 28, 2022, D.J.'s dashboard account was locked or disconnected., and

e. D.J. provided the following URL where other victims of Scorpio Group LLC posted about their experience: https://www.scampulse.com/scorpio-group-reviews.

64. Victim "U.G.", a resident of Texas, reported to the following to IC3:

a. On or about January 14, 2022, U.G. was offered a job as a "Logistics inspector" by the company Navois USA LLC. The company provided U.G. a domain to access the employee online dashboard, account-navois.com.,

b. U.G. was hired to make purchases via their own credit card and was told that the purchase payments would be reimbursed. U.G. spent approximately $32,000, which was not reimbursed by the subject company.,

c. U.G. was contacted from multiple email addresses that followed the convention firstname(dot)lastname(at)companynameemail.com with titles such as Manager Shipping Department. For example, T[redacted] D[redacted] emailed U.G. as the Manager Shipping Department from email address T[redacted](at)navoisusaemail.com.,

65. Victim "D.M.", a resident of Nevada, reported the following to IC3:

a. On or about January 11, 2022, D.M.was offered a Remote Logistics job with Navois USA. D.M. first found the job listed on Indeed.com. D.M. was hired to receive packages,

then send them out on the same day using an outgoing shipping label provided by the company (i.e., the victim was hired as a "reshipper").

b. D.M. was told the position salary was $2200/month plus an additional $50 for each successful delivered package. The company provided D.M. a domain to access the employee online dashboard, navois-account.com. D.M. provided the subject company with PII, such as name, address, and social security number.

c. On or about January 13, 2022, D.M. received the first of eleven total packages. On February 11, 2022, one month after D.M. began working at Navois US, the dashboard account was locked or disconnected. The subjects have D.M.'s name, address, social security number, phone number, photo identification, and bank account information.

d. D.M. was contacted from multiple email addresses that followed the convention firstname(dot)lastname(at)companynameemail.com with titles such as Supervisor Shipping Department. For example, D[redacted] emailed D.M. as the Manager Shipping Department from email address d[redacted](at)navoisusaemail.com.

e. The company provided a link to its official website and to the Nebraska Secretary of State's website to verify the company's legitimacy.

66. The aforementioned victim complaints are intended to present the basic nature of the scam and are not an exhaustive presentation of complaints. Members of the investigative team and I reviewed the IC3 complaints and observed the following repeating commonalities and characteristics of the scam, as reported by victims:

a. Complainants believed they had applied for work-at-home employment,

b. Complainants were instructed to receive shipments, repackage/relabel shipments, and reship those same items to another address,

c. Complainants believed they would be paid for this work at their negotiated rate,

d. Complainants were directed to log-in to one or more of the domain names identified in the Cloudflare records,

e. Complainants used one or more of the domain names identified in the Cloudflare records to facilitate the receiving and reshipment of packages and communicate with unknown persons,

f. Complainants never received full compensation for the work they completed, and

g. Complainants reported they were unknowingly involved in scam.

Federal Trade Commission Complaints

67. The Federal Trade Commission takes reports from the public concerning scams in the marketplace. These reports are stored in the Consumer Sentinel Network, hereinafter "Sentinel", a secure online database available only to law enforcement. Sentinel records identified fifty-six (56) complaints that referenced the domain names identified in the Cloudflare records. These reports were received between January 6, 2021 and March 12, 2022. The complainants reported home addresses in twenty different states. Members of the investigative team and I reviewed the Sentinel complaints and observed the following repeating commonalities and characteristics of the scam, as reported by victims:

a. Complainants believed they had applied for work-at-home employment,

b. Complainants were instructed to receive shipments, repackage/relabel shipments, and reship those same items to another address,

c. Complainants believed they would be paid for this work at their negotiated rate,

d. Complainants were directed to log-in to one or more of the domain names identified in the Cloudflare records,

e. Complainants used one or more of the domain names identified in the Cloudflare records to facilitate the receiving and reshipment of packages and communicate with unknown persons,

f. Complainants never received full compensation for the work they completed, and

g. Complainants reported they were unknowingly involved in scam.

68. Based on the repeating patterns found in the FTC and IC3 complaints, I believe each of the domain names identified in the Cloudflare records are being created, maintained, and operated by one or more unknown persons involved in the facilitation of the SUBJECT OFFENSES.

THE SUBJECT DOMAIN NAMES

69. As described above, the SUBJECT DOMAIN NAMES were used by unknown persons to facilitate identity theft with the intent to obtain stolen goods, in the Eastern District of Missouri and elsewhere, in order to evade detection from law enforcement throughout the United States.

70. The SUBJECT DOMAIN NAMES were utilized to electronically transmit fictitious identification documents, transmit shipping labels with victim's names, track stolen goods as they are transported throughout the United States, and communicate with various known and unknown parties.

71. A search of publicly available WHOIS domain name registration records revealed that the SUBJECT DOMAIN NAMES were registered by one of the following registrars:

a. Dynadot, LLC, a company headquartered in San Mateo, California,

b. Eranet International Limited, a company headquartered in Hong Kong

c. PDR Ltd d/b/a Public Domain Registry, a company headquartered in India

d. Reserved-Internet Assigned Numbers, a company headquartered in Los Angeles, California, and

e. Tucows Domains Inc., a company headquartered in Canada.

72. The use of registrars outside of the United States requires the seizure of the SUBJECT DOMAIN NAMES from the top-level registry, not the individual registrars.

73. The top-level domain for all of the SUBJECT DOMAIN NAMES is Verisign Inc. (hereinafter "Verisign"). Verisign currently manages all ".com" domains.

SEIZURE PROCEDURE

74. As detailed in Attachment B, upon execution of the seizure warrant, the registry for the ".com" top-level domain, Verisign Inc., shall be directed to restrain and lock the SUBJECT DOMAIN NAMES pending transfer of all right, title, and interest in the SUBJECT DOMAIN NAMES to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAMES cannot be made absent court order or, if forfeited to the United States, without prior consultation with USPIS and FBI.

75. In addition, upon seizure of the SUBJECT DOMAIN NAMES by USPIS and FBI, Verisign will be directed to associate the SUBJECT DOMAIN NAMES to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which the SUBJECT DOMAIN NAMES will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

CONCLUSION

76. Based on the information contained in this affidavit, I submit that there is probable cause to believe that the SUBJECT DOMAIN NAMES are used in and/or intended to be used in facilitating and/or committing the SUBJECT OFFENSES. Accordingly, the

SUBJECT DOMAIN NAMES are subject to forfeiture to the United States pursuant to 18 U.S.C. 1028(b)(5) and 1029(c)(1)(C), and I respectfully request that the Court issue a seizure warrant for the SUBJECT DOMAIN NAMES.

77. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the SUBJECT DOMAIN NAMES for forfeiture. By seizing the SUBJECT DOMAIN NAMES and redirecting it to another website, the Government will prevent third parties from acquiring the name and using it to commit additional crimes. Furthermore, seizure of the SUBJECT DOMAIN NAMES will prevent third parties from continuing to access these websites.

78. Because the warrant will be served on Verisign, which controls the SUBJECT DOMAIN NAMES, at a time convenient to it, the registry will transfer control of the SUBJECT DOMAIN NAMES to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

79. Finally, and in order to protect the ongoing investigation and in consideration that much of the information set forth above is not otherwise publicly available, I respectfully request that this Affidavit be filed and kept under seal until further order of this Court.

Respectfully submitted,

Peter Dyer
Postal Inspector
U.S. Postal Inspection Service

Subscribed to and sworn before me on this 21st day of October, 2022.

Patricia L. Cohen
HONORABLE PATRICIA L. COHEN
United States Magistrate Court Judge

ATTACHMENT A

The SUBJECT DOMAIN NAMES that are to be seized include:

Ref	*SUBJECT DOMAIN NAME*
1	account-navois.com
2	amari-dash.com
3	control-scorpio.com
4	costa-account.com
5	dash-amari.com
6	dashboard-zim.com
7	dash-egreen.com
8	dash-orient.com
9	dash-satori.com
10	dash-spt.com
11	egreen-dash.com
12	main-sgl.com
13	navois-account.com
14	orient-dash.com
15	satori-dash.com
16	scorpio-control.com
17	spt-dash.com
18	zim-dash.com

ATTACHMENT B

IT IS ORDERED that, with respect to SUBJECT DOMAIN NAMES, as listed in Attachment A, Verisign, who is the domains' registry, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN NAMES:

1. Take all reasonable measures to redirect the domain names to substitute servers controlled by the USPIS, by associating the SUBJECT DOMAIN NAMES to the following authoritative name-server(s) **[OR by redirecting traffic to the Subject Domain Name to the following IP address**]:

a. NS1.SEIZEDWEBSITE.COM (associated IP Address 66.212.148.115)

b. NS2.SEIZEDWEBSITE.COM associated IP Address 66.212.148.116); and/or

c. Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to the Subject Registry.

2. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable;

3. Prevent any further modification to, or transfer of, SUBJECT DOMAIN NAMES pending transfer of all right, title, and interest in SUBJECT DOMAIN NAMES to the United States upon completion of forfeiture proceedings, to ensure that changes to the Subject Domain Name cannot be made absent court order or, if forfeited to the United States, without prior consultation with the USPIS and FBI.

4. Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

5. The Government will display a notice on the website to which the Subject Domain Name will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

This domain has been seized by the U.S. Postal Inspection Service and the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. § 981(b) and 21 U.S.C. § 853(f) by the United States District Court for the Eastern District of Missouri as part of a law enforcement action by the U.S. Postal Inspection Service and Federal Bureau of Investigation and the U.S. Attorney's Office for the Eastern District of Missouri.

I. Seizure Procedure

A. The seizure warrant will be presented in person or transmitted via facsimile or email to personnel of the domain name registry listed in Section II ("Subject Registry") who will be directed, for the domain names listed in Section IV ("Subject Domain Names") for which it serves as the top-level domain registry, to make any changes necessary to restrain and lock the domain name pending transfer of all rights, title, and interest in the Subject Domain Name to the United States upon completion of forfeiture proceedings.

B. Upon seizure of the Subject Domain Names, the Subject Registry shall point the Subject Domain Names to the IP address(es) identified in Attachment B, at which the Government will display a web page with the following notice:

This domain has been seized by the U.S. Postal Inspection Service and the Federal Bureau of Investigation in accordance with a seizure warrant issued pursuant to 18 U.S.C. § 981(b) and 21 U.S.C. § 853(f) by the United States District Court for the Eastern District of Missouri as part of a law enforcement action by the U.S. Postal Inspection Service and Federal Bureau of Investigation and the U.S. Attorney's Office for the Eastern District of Missouri.

C. Upon seizure of the Subject Domain Names, the Subject Registry shall take all steps necessary to restrain and lock the domain at the registry level to ensure that changes to the subject domain names cannot be made absent a court order or, if forfeited to the United States government, without prior consultation with the U.S. Postal Inspection Service and the Federal Bureau of Investigation. The DNS record should be altered to remove any applicable name servers.

D. Upon seizure of the Subject Domain Names, the Subject Registrars shall modify any records, databases, tables, or documents that are used by the Subject Registrars to identify the

owner of the Subject Domain Names to reflect the seizure of the Subject Domain Names. These changes relate to the following records, if they exist:

1. The "Technical Contact" and "Administrative Contact" fields will reflect the following information:

a) Name: United States Postal Inspection Service

b) Address: 475 L'Enfant Plaza SW, Washington, DC 20260

c) Country: USA

d) Telephone: 8778762455

e) Email: seizeddomain@uspis.gov

f) Fax: 2026362381

2. Any remaining fields will be changed so they do not reflect any individual or entity.

E. The Subject Registry shall take any steps required to propagate the changes detailed in Section D to any applicable DNS servers.

II. Subject Registry

Verisign, Inc.

12061 Bluemont Way

Reston, Virginia 20190

III. Subject Registrars: SEE ATTACHMENT A

IV. Subject Domain Names: SEE ATTACHMENT A

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Seizure of Eighteen (18) ".Com" Domain Names, further described in Attachment A	)))))	Case No. 4:22MJ6246 PLC

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property as being subject to forfeiture to the United States of America. The property is described as follows:

Eighteen (18) ".Com" Domain Names, further described in Attachment A,

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property for criminal and civil forfeiture, and that an order under Title 21, United States Code, Section 853(e) may not be sufficient to assure the availability of the property for forfeiture.

YOU ARE COMMANDED to execute this warrant and seize the property on or before November 4, 2022
(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to the Honorable Patricia L. Cohen, United States Magistrate Judge.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41

Date and time issued: October 21, 2022 at 11:10 a.m.

Patricia L. Cohen
Judge's signature

City and state: St. Louis, Missouri

Honorable Patricia L. Cohen, U.S. Magistrate Judge
Printed name and title

RETURN

DATE WARRANT RECEIVED	DATE AND TIME WARRANT EXECUTED	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH

INVENTORY MADE IN THE PRESENCE OF

INVENTORY OF PERSON OR PROPERTY TAKEN PURSUANT TO THE WARRANT

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

_____

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

IN THE MATTER OF THE SEIZURE OF: Eighteen (18) ".Com" Domain Names, further described in Attachment A,	)	No.: 4:22MJ6246 PLC **[FILED UNDER SEAL]**

APPLICATION TO SEAL SEIZURE WARRANT

Comes now the United States of America, by and through its attorneys, Sayler Fleming, United States Attorney for the Eastern District of Missouri, and Derek J. Wiseman, Assistant United States Attorney for said District, and moves this Court for an order directing that the seizure warrant, application, and affidavit entered by this Court be sealed until April 21, 2023.

In support of this Motion, the government provides the following facts establishing that (a) the government has a compelling interest in sealing the documents in question which outweighs the public's qualified First Amendment right of access to review those documents; and (b) no less restrictive alternative to sealing is appropriate or practical.

The facts submitted in the affidavit in support of the instant application have been determined as part of an ongoing investigation. Disclosure of the contents of the affidavit for the seizure warrant would identify individuals under investigation but not yet charged with an offense, and may also place the individuals identified in the affidavit in danger.

WHEREFORE, for the reasons stated above, the Government respectfully requests that the seizure warrant, along with its application, affidavit, and return, be sealed until April 21, 2023.

SAYLER FLEMING
United States Attorney

/s/ *Derek J. Wiseman*
DEREK J. WISEMAN, #67257(MO)
Assistant United States Attorney
111 South 10th Street, Room 20.333
St. Louis, Missouri 63102
(314) 539-2200

Dated: October 21, 2022